UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

THOMAS ROGER WHITE, JR., and PATRICIA CAULEY, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

SAMSUNG ELECTRONICS AMERICA, INC., and SONY ELECTRONICS INC,

Defendants.

Case No. 17-1775 (MCA) (SCM)

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

INTRODUCTION

As detailed in Plaintiffs' Second Amended Class Action Complaint ("Complaint" or "Compl."), Defendants' Smart TVs secretly intercept, track and store everything consumers watch, everything consumers say, as well as the specific identifiers (and thus the real world location) of other electronic devices that consumers connect to their Smart TVs and/or Wifi. Compl. ¶¶ 38-67. Defendants then unilaterally sell consumers' private information, sensitive viewing histories, personal preferences, contents of conversations, and other personally-identifying information (i.e., consumers' "digital identities") to third-party advertisers and data brokers, who in turn target advertisements to consumers' other electronic devices (based on the confidential consumer-information provided by Defendants). Compl. ¶¶ 2-5, 42, 43, 68. Defendants do this without first obtaining informed consent from consumers, and Defendants are able to track and record consumers indefinitely. Compl. ¶¶ 39, 44.[1]

Defendants also secretly collect and disclose to third parties consumers' Internet Protocol (IP) addresses, media access control (MAC) addresses, and zip codes. In this advanced technological age, this data and the other personally identifiable information disclosed by Defendants to third parties can easily be used by an ordinary person to pinpoint a consumers' physical location and electronic identity. See infra.

In essence, Defendants' business model treats all consumers as Defendants' very own Nielsen family. The critical difference is that, unlike Defendants' Smart TV consumers, Nielsen family members *agree* to share their viewing habits and are *paid* for their participation.[2]

Defendants do not even attempt to deny that they siphon, store, and transmit consumers' proprietary, personally identifiable information, or that they do so without first obtaining informed consent from consumers. Rather, Defendants simply argue that they are not subject to

---

[1] "Samsung's 'Always On' Voice Recorders
When the voice recognition feature on a Samsung Smart TV is enabled, everything a user says in front of the Samsung Smart TV in recorded and transmitted over the internet to a third party regardless of whether it is related to the provision of the service." Compl. At ¶ 1, note 1.

[2] Defendants lure consumers with features such as video libraries on-demand, Netflix, Amazon, Hulu, Pandora, and other enticing applications and, once consumers take the bait, Defendants are then able *to forever* follow these unsuspecting consumers deep into the private, confidential areas of their lives.

any of the laws that would enable the Court to stop the sophisticated snare Defendants have laid down for unsuspecting consumers.

The New Jersey Consumer Fraud Act ("NJCFA" or "CFA"), however, is not so meek. The statute was enacted to be one of the strongest consumer protection laws in the nation and it explicitly prohibits - not only fraud - but *any and all* unfair, deceptive and/or unconscionable business practices in New Jersey. The CFA is to be applied liberally by the courts, and the statute has been held to protect consumers from unfair business practices even when a merchant acts in good faith and even if no person was in fact misled or deceived thereby. Accordingly, Defendants violations of the CFA renders them liable for damages.[3]

Furthermore, the Third Circuit has specifically held that, in the context of a privacy violation by a defendant (like here), "improper dissemination of information can itself constitute a cognizable injury." In re Horizon Healthcare Servs., Inc. Data Breach Litig., 846 F.3d 625, 638-641 (3d Cir. 2017) (J. Shwartz, concurring) (citing Spokeo, Inc. v. Robins, 136 S.Ct. 1540 (2016) ("The common law has historically recognized torts based upon the invasions of privacy and permitted such claims to proceed in the absence of actual damages."). As such, Plaintiffs and the Class members have suffered a loss from Defendants' unlawful interception and dissemination of Plaintiffs' private information.

Additionally, federal privacy and other statutes (including the Video Privacy Protection Act and the Federal Wiretap Act) also limit Defendants' legal right to collect or disclose consumers' personal and/or identifying information without informed consent, and Defendants' failure to secure that informed consent from Plaintiffs and the Class also renders them liable for damages.

FACTS

Defendants are amongst the largest manufacturers in the world of "Smart TVs," cutting-edge televisions equipped with integrated software that enables consumers to access, amongst other things, the internet and instant, on-demand video services. Compl. ¶¶ 35-36. Defendants' business model, however, is much more than selling TVs. In reality, due to fierce

[3] Defendants' unlawful conduct also violates the Florida Deceptive and Unfair Trade Practices Act, 15 U.S.C. § 45, the Cable Communications Policy Act, 47 U.S.C. § 631(b), and the Children's Online Privacy Protection Act, 16 C.F.R. § 312.3. See infra.

market competition, Defendants reap extremely slim profit margins on TV sales. To offset this, Defendants use Automatic Content Software ("ACS") to intercept, in real time, consumers' viewing data, watching habits, MAC and IP addresses, voice contents, and other personally identifiable information, and Defendants then sell this valuable, confidential-information to third parties. Compl. ¶¶ 6, 38-53.

Defendants' Smart TVs stream video and other content to consumers, and allow consumers to access WiFi networks to gain access and watch various forms of audio and visual entertainment online, as well as to find access to online news, weather, and entertainment sources. Compl. ¶ 34. To accomplish this, Defendants' Smart TVs are delivered to consumers with many preinstalled applications, and other applications are uploaded by Defendants to their Smart TVs. These include such popular internet applications as Netflix, YouTube, Amazon, Pandora, Hulu, Twitter, and more. The list is ever-growing. Compl. ¶ 36.

Defendants intercept, aggregate, and store data for most of the content viewed on their Smart TVs – and also the other devices connected to the consumers' Wifi (such as cable and satellite providers, gaming consoles, DVD players, and other sources). Compl. ¶¶ 44, 50, 51. Defendants then sell this data to third-party advertisers and media content providers, who also use (and store) this private information to target consumers. See, e.g., Compl. ¶¶ 42, 51-53. Throughout the process, Defendants also collect a wide array of additional information about consumers' watching habits and views, including their IP addresses, zip codes, online services used, MAC addresses, and much more identifying information. Compl. ¶¶ 6, 38-53. The date and time of users viewing and search history is also collected,and a data "fingerprint" is created by Defendants for each individual Smart TV user in the home. Compl. ¶46-48, 52-53; Cognitive Network's Automatic Content Software materials (attached as Exhibit 4 to the Complaint).

Defendants accomplish their pirating of consumers' confidential information and voice recordings by employing the services of outside, third-party companies, such as Cognitive Networks, whose only business purpose is to accomplish exactly what Plaintiffs have alleged here. Compl. ¶¶ 54-58. See also Cognitive Network's Automatic Content Software materials (attached as Exhibit 4 to the Complaint).

The data and voice collection by Defendants also allows that information to be used by Defendants to identify specific people in the home (including children), compl. ¶49, and connect them with what they have been watching and where they live. For example, Plaintiffs allege that Defendants scan consumers' Wifi system. Compl. ¶¶ 43. 50. Plaintiffs also allege that Defendants video-streaming platforms disclose substantial, extensive information about Plaintiffs' and consumers' "digital identities"; namely, consumers' video-viewing history, voice content, computer addresses (MAC and IP), and other information about other devices connected to the same Wifi network. See Compl. ¶¶ 43, 45-49, 53. Further, users can be asked by certain applications on Smart TVs to sign up for services requiring their name and email address, which makes it especially easy for to identify consumers' viewing habits and location.

The named Plaintiffs in this case bought Defendants' Smart TVs with no inkling of the fact that Defendants would be monitoring and disclosing everything they watch and say – let alone that Defendants would be selling and transmitting their private, confidential, identifying information to third parties, for profit. Compl. ¶¶ 12, 59-67. Although, like every purchaser of a Smart TV, Plaintiffs examined Defendants' packaging and marketing when they were shopping for their Smart TVs and noted features such as the TVs' ability to connect to the internet and stream content from many sources, Plaintiffs did not see – because Defendants failed to properly disclose – any indication that their viewing data, personally-identifiable information, and voice content would be collected, stored by Defendants, and sold to third parties. Id. With Plaintiffs having no idea of the scheme Defendants had cooked-up to invade, store, and sell their private and identifying information (and because consumers were not reasonably provided with all the facts to make an informed decision), Plaintiffs did not – and could not – give informed consent to the unlawful collection by Defendants of their private information and/or Defendants' disclosure of this information to third parties for profit.

Had Plaintiffs and the Class members known the truth, they would have not purchased Defendants' Smart TVs, or would have paid substantially less. Compl. ¶ 12.

Defendants Do Not Attempt To Obtain Informed Consent From Consumers

Nowhere in the packaging or marketing of Defendants' Smart TVs do Defendants disclose its data and voice collection practices (and that Defendants sell that information to third

parties, who also store that sensitive information). Compl. ¶¶ 61-62. Even though it would be simple and no-cost for Defendants to alert consumers on the television box itself (i.e, *prior* to the purchase of the TV by the consumer) that Defendants intercept and store indefinitely consumers' highly sensitive, personal and confidential information and voices (and that Defendants then sell this confidential information to third parties), Defendants do not print this material information on the television box. Even though it would be simple and no cost for Defendants to put in bold print (or any print) in the instruction manual in the box that Defendants intercept and store indefinitely consumers' highly-sensitive, personal and confidential information and voices (and that Defendants then sell this confidential information to third parties), Defendants do not print this material information on in the instruction manual in the box.

Further, even though it would be simple and no-cost for Defendants to put a conspicuous, separate and bold "Privacy Information Sheet" in the box that explains how and why Defendants collect (and store indefinitely) consumers' highly-sensitive, personal and confidential information and voices (and that Defendants then sell this confidential information to third parties), Defendants do not include any conspicuous "Privacy Information Sheet" inside the box. See Compl. ¶¶ 9, 14 ("Had Plaintiffs known the truth about Defendants' data collection and tracking software, they would not have purchased Defendants' Smart TVs or would have paid substantially less for them.").

As such, it is clear that the Defendants have not taken reasonable steps to ensure that they obtained informed consent from Plaintiffs and the Class.

ARGUMENT

I. The New Jersey Consumer Fraud Act

A. The NJCFA Is To Be Applied Liberally

The enactment of the New Jersey Consumer Fraud Act ("NJCFA" or "CFA") was aimed at "unlawful sales and advertising practices designed to induce customers to purchase merchandise."*Daaleman v. Elizabethtown Gas Co., 77 N.J. 267, 270, 390 A.2d 566 (1978)*. The statute "was intended to be one of the strongest consumer protection laws in the nation" and

"should be construed liberally in favor of consumers." *New Mea Const. Corp. v. Harper, 203 N.J. Super. 486, 501-02* App. Div.); *Cox v. Sears Roebuck & Co., 138 N.J. 2, 15 (1994)*. See also *Huffmaster v. Robinson, 221 N.J. Super. 315, 319 (Law Div. 1986)*. The CFA is a remedial statute and its remedies in private actions are "not only to make whole the victim's loss, but also to punish the wrongdoer and to deter others from engaging in similar fraudulent practices." *Furst v. Einstein Moomjy, Inc., 182 N.J. 1, 12 (2004);* accord, *Thiedemann v. Mercedes-Benz USA, LLC, 183 N.J. 234, 246 (2005); Cox, 138 N.J. at 21; Lettenmaier v. Lube Connection, Inc., 162 N.J. 134, 139 (1999).*

In enacting the NJCFA, the New Jersey Legislature recognized that:

> [T]he deception, misrepresentation and unconscionable practices engaged in by professional sellers seeking mass distribution of many types of consumer goods frequently produce an adverse effect on large segments of disadvantaged and poorly educated people, who are wholly devoid of expertise and least able to understand or to cope with the "sales oriented," "extroverted" and unethical solicitors bent on capitalizing upon their weakness, and who therefore most need protection against predatory practices.

Kugler v. Romain, 58 N.J. 522, 536 279 A.2d 640 (1971).

Accordingly, by way of the CFA, New Jersey can enforce its "powerful incentive to insure that local merchants deal fairly with citizens of other states and countries." *Boyes v. Greenwich Boat Works, Inc., 27 F. Supp. 2d 543, 547 (D. N.J. 1988).*

B. Plaintiffs Have Stated A Claim Under the NJCFA

The New Jersey Supreme Court has interpreted a CFA claim to include "three elements: (1) unlawful conduct . . . ; (2) an ascertainable loss . . . ; and (3) a causal relationship between the defendants' unlawful conduct and the plaintiff's ascertainable loss." *Int'l Union of Operating Eng'rs Local No. 68 Welfare Fund v. Merck & Co., Inc., 192 N.J. 372, 389, 929 A.2d 1076 (2007)* (quoting *New Jersey Citizen Action v. Schering-PloughCorp., 367 N.J. Super. 8, 12-13, 842 A.2d 174 (App. Div.), certif. denied, 178 N.J. 249, 837 A.2d 1092 (2003))*. Plaintiffs' allegations as set forth in the Complaint satisfy each of these elements.

1. Unlawful Conduct Under The CFA

The NJCFA defines an "unlawful conduct" broadly as:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . . whether or not any person has in fact been misled, deceived or damaged thereby.
> .

N.J. Stat. Ann. § 56:8-2.

Furthermore, the conduct specified in the NJCFA as amounting to an unlawful practice is disjunctive. *Id. at 19.* Therefore, "[p]roof of **any one** of those acts or omissions or of a violation of a regulation will be sufficient to establish unlawful conduct under the Act." Id. *Cox v. Sears Roebuck & Co., 138 N.J. 2, 13 647 A.2d 454 (N.J. 1994)* (emphasis added).

The New Jersey Supreme Court in *Cox* further explained what constitutes "unlawful conduct" under the NJCFA:

> To violate the Act, a person must commit an "unlawful practice" as defined in the legislation. Unlawful practices fall into three general categories: affirmative acts, knowing omissions, and regulation violations. The first two are found in the language of *N.J.S.A.* 56:8-2, and the third is based on regulations enacted under *N.J.S.A.* 56:8-4. **A practice can be unlawful even if no person was in fact misled or deceived thereby**. *D'Ercole Sales, supra, 206 N.J. Super. at 22, 501 A.2d 990; Skeer, supra, 187 N.J. Super. at 470, 455 A.2d 508.* The capacity to mislead is the prime ingredient of all types of consumer fraud. *Fenwick v. Kay Am. Jeep, Inc., 72 N.J. 372, 378, 371 A. 2d 13 (1977).*

Id. (emphasis added). Moreover, the CFA protects consumers from unfair practices "even when a merchant acts in good faith." Id. at 16.[4]

Under the NJCFA, "[u]nlawful *affirmative acts* consist of unconscionable commercial practice, fraud, deception, false promise, false pretense, and misrepresentation." *Estate of Knoster v. Ford Motor Co., No. 01-3168, 2008 U.S. Dist. LEXIS 103342, 2008 WL 5416399,* at *8 (D.N.J. Dec. 22, 2008) (citing *Thiedemann v. Mercedes-Benz USA, LLC, 183 N.J. 234, 872 A. 2d 783, 7.*91 (N.J. 2005) (emphasis added). And when the alleged consumer-fraud violation consists of affirmative acts (as in the instant case), under the NJCFA, intent is not an essential element and the plaintiff need *not* prove that the defendant intended to commit an unlawful act. *Chattin v. Cape May Greene, Inc., 124 N.J. 520, 522, 591 A.2d 943 (1991)* (Stein, J. concurring).[5]

Moreover, the CFA's "unconscionable commercial practice" language is a "catch-all" provision that is not defined, but is:

> an amorphous concept obviously designed to establish a broad business ethic. The framers of the Code naturally expected the courts to interpret it liberally so as to effectuate its purpose, and to pour content into it on a case-by-case basis. . . . [T]he Legislature intended to broaden the scope of responsibility or unfair business practices by stating in Section 2 that the use of any of the described practices is unlawful 'whether or not any person [the consumer] has in act been misled, deceived or damaged thereby.'"

Kugler v. Romain, 58 N.J. at 544, 279 A.2d at 640. Thus, the CFA is not only aimed at con men, but is "designed to promote the disclosure of relevant information to enable the consumer to make intelligent decisions in the selection of products and services." *Leon v. Rite Aid Corp., 340*

[4] The CFA also expressly covers and protects indirect purchasers, in that it defines merchandise as "any objects, wares, goods, commodities, services or anything offered, directly or indirectly, to the public for sale." N.J.S.A. 56:8-1(c). The statute also broadly defines the term "sale" to include "any sale, rental or distribution, offer for sale, rental or distribution or attempt directly or indirectly to sell, rent or distribute." N.J.S.A. 56:8-1(e).

[5] The core of Defendants' unlawful conduct in this case consists of *affirmative acts*; namely, intercepting, storing indefinitely, and transmitting to third parties for profit Plaintiffs' confidential, personally identifiable information.

N.J. Super. 462, 471 (App. Div. 2001). See also *Perth Amboy Iron Works, Inc. v. American Home Assurance Co., 226 N.J. Super. 200, 209 (App. Div. 1988)*.

2. Plaintiffs Have Adequately Pled Defendants' Unlawful Conduct

Plaintiffs have alleged that Defendants' unlawful conduct consists of, amongst other things: (i) intercepting and storing indefinitely consumers' confidential information and voice recordings by means of their Smart TVs; (ii) unilaterally selling consumers' private information, sensitive viewing histories, personal preferences, contents of conversations, and other personally-identifying information (i.e., consumers' "digital identities") to third-parties; and (iii) failing to obtain informed consent from consumers before doing so.

Plaintiffs have properly alleged that "the CFA defines 'merchandise' as 'any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale.' N.J. Stat. Ann. § 56:8-1(c). . . . and [that] [a]t all relevant times, Defendants have engaged in the advertisement, offering for sale and sale of merchandise within the meaning of N.J. Stat. Ann. § 56:8-1(c), specifically Defendants' Smart TVs and related services." Compl. §§ 117-118. Plaintiffs further allege that: (i) "Defendants use A[utomatic] C[ontent] S[oftware] technology to comprehensively collect the sensitive television viewing activity of consumers or households across cable or broadband services, set-top boxes, external streaming devices, DVD players, and over-the-air broadcasts, on a second-by-second basis and store this viewing data indefinitely"; compl. §119; (ii) "Defendants provided this viewing data to third parties, which used it to track and target advertising to individual consumers across devices;" compl. §120 and (iii) "Defendants engaged in these practices through a medium that consumers would not expect to be used for tracking, without consumers' consent; namely, consumers' own Smart TVs." Id.

Plaintiffs also properly allege the other requisite elements of their CFA claims, see infra, and properly allege that "Defendants' continued utilization of unlawful and unconscionable marketing practices, and their continuing practice of monitoring, tracking, and reporting viewing habits and personally identifiable information to unauthorized third parties, without consent, constitutes a deceptive act or practice in violation of the CFA . . . . [and] such is also an unconscionable commercial practice in violation of the CFA. Each instance of Defendants' unfair tracking and/or recording of consumers constitutes a separate violation under the CFA,

N.J. Stat. Ann. § 56:8-2." Compl. §121-122, 146. Plaintiffs further allege that Defendants violated the CFA because they "failed to adequately disclose that the ACS feature of their Smart TVs comprehensively collected and shared consumers' television viewing activity from cable boxes, DVRs, streaming devices, and airwaves, which Defendants then provided on a household-by-household basis to third parties (and then to "second-level" third parties)." Compl. §135.

3. Plaintiffs Have Adequately Plead Ascertainable Loss Under the NJCFA

The CFA authorizes a statutory remedy for "[a]ny person who suffers any ascertainable loss of moneys or property, real or personal, as a result of the use or employment by another person of any method, act, or practice declared unlawful under this act." *N.J.S.A. 56:8-19*. Although Defendants attempt to argue that Plaintiffs' CFA claims here are intangible, they are incorrect because Plaintiffs in this case have suffered substantial loss as a result of Defendants' unlawful conduct.[6]

First, any value associated with a consumer's private information is owned by the consumer; not Defendants. Because Defendants sold consumers' personal information without informed consent, the monies that Defendants reaped from unlawfully selling Plaintiffs' and the Class' private information is loss to Plaintiffs. Discovery will clearly help determine how much monies Defendants earned through their scheme and, by extension, how much loss to Plaintiffs occurred by means of Defendants' privacy violations.

Moreover, the Supreme Court of New Jersey has already determined that a Plaintiff necessarily suffers an injury-in-fact based on the loss of privacy. As succinctly explained by the Third Circuit in In re Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 642-43 (3d Cir. 2017) (holding "improper dissemination of information can itself constitute a cognizable injury"):

> [T]he Spokeo Court identified two approaches for determining whether an intangible injury is sufficient to constitute an injury in

[6] Plaintiffs have specifically alleged that Defendants' privacy violations caused Plaintiffs' loss. See Compl. §§126, 140, 143, 173

> fact. Maj. Op. at 23 (citing *Spokeo*, 136 S. Ct. at 1549). Under the first approach, a court considers history and asks whether the intangible harm is closely related "to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." Id. at 1549; Maj. Op. at 23. If so, "it is likely sufficient to satisfy the injury-in-fact element of standing." Maj. Op. at 23 (citing *Spokeo*, 136 S. Ct. at 1549). . . . The common law has historically recognized torts based upon invasions of privacy and permitted such claims to proceed even in the absence of proof of actual damages. *See*, *e.g.*, *Pichler v. UNITE*, 542 F.3d 380, 399 (3d Cir. 2008) (citing *Doe v. Chao*, 540 U.S. 614, 621 n.3, 124 S. Ct. 1204, 157 L. Ed. 2d 1122 (2004)); Restatement (Second) Torts §652A (2016) (stating that "[o]ne who invades the right of privacy of another is subject to liability for the resulting harm to the interest of the other"). While Plaintiffs do not allege that the laptop thieves looked at or used their PII and PHI, Plaintiffs lost their privacy once it got into the hands of those not intended to have it. Cf. *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577 n.5 (3d Cir. 1980)(observing that "[p]rivacy . . . is control over knowledge about oneself" (citation omitted)). . . .
>
> Our Court has embraced the view that an invasion of privacy provides a basis for standing. *In In re Google Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015), and *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262 (3d Cir. 2016), Google and Nickelodeon were alleged to have invaded the plaintiffs' privacy by placing cookies into the plaintiffs' computers, which allowed the companies to monitor the plaintiffs' computer activities. In these cases, the injury was invasion of privacy and not economic loss, and thus the standing analysis focused on a loss of privacy. *In re Nickelodeon*, 827 F.3d at 272-73; *In re Google*, 806 F.3d at 134. Although the perpetrators of the invasion of privacy here are the laptop thieves and in Google and Nickelodeon the invaders were the defendants themselves, the injury was the same: a loss of privacy. Thus, those cases provide a basis for concluding Plaintiffs here have suffered an injury in fact based on the loss of privacy.

846 F.3d at 642-43 (J. Shwartz, concurring) (emphasis added).

Additionally, a second approach in determining whether a privacy violation causes loss is for the court to consider whether the legislature "expressed an interest to make a injury redressable." Id. Here, the Plaintiffs have an even *stronger* basis for claiming that they suffered

harm than did the plaintiffs in Google and Nickelodeon because, here, in addition to Defendants intercepting, storing, and transmitting Plaintiffs' confidential, personally identifiable information, Defendants also recorded Plaintiffs' spoken words and also transmitted that information over the internet to third parties. Compl. §§ 39, 42, note 1.

In In re Horizon Healthcare, the Third Circuit further explained why a Plaintiff who is the victim of a privacy violation (as in the instant case) suffers loss:

> *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015), certain internet users brought an action against internet advertising providers alleging that their placement of so-called "cookies" — i.e. small files with identifying information left by a web server on users' browsers — violated a number of federal and state statutes, including the Stored Communications Act. Id. at 133. The defendants argued that because the users had not suffered economic loss as a result of the violations of the SCA, they did not have standing. Id. at 134. **We emphasized that, so long as an injury "affect[s] the plaintiff in a personal and individual way," the plaintiff need not "suffer any particular type of harm to have standing."** Id. (citation and internal quotation marks and citation omitted). Instead . . . the [privacy] invasion . . . creates standing," even absent evidence of actual monetary loss. Id. (citation and internal quotation marks omitted)
>
> We then reaffirmed Google's holding in *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262 (3d Cir. 2016). That case involved a class action in which the plaintiffs alleged that Viacom and Google had unlawfully collected personal information on the Internet, including what webpages the plaintiffs had visited and what videos they watched on Viacom websites. Id. at 267. We addressed the plaintiffs' basis for standing, relying heavily upon our prior analysis in *Google*, id. at 271-272, saying that, **"when it comes to laws that protect privacy, a focus on economic loss is misplaced."** Id. at 272-73 (citation and internal quotation marks omitted). Instead, "the unlawful disclosure of legally protected information" constituted "a clear de facto injury." Id. at 274. . . . .
>
> In light of those two rulings, our path forward in this case is plain. The Plaintiffs here have at least as strong a basis for claiming that they were injured as the plaintiffs had in Google and Nickelodeon.

846 F.3d at 636 (3d Cir. 2017) (emphasis added).

As the history and interpretation of the NJCFA makes clear, see supra, the New Jersey Legislature intended the NJCFA to be "one of the strongest consumer protection laws in the nation" and "should be construed liberally in favor of consumers." New Mea Const. Corp. v. Harper, 203 N.J. Super. 486, 501-02 App. Div.); Cox v. Sears Roebuck & Co., 138 N.J. 2, 15 (1994). Accordingly, just as in Nickelodeon, Google, and Horizon Healthcare, in this case, in determining whether Plaintiffs suffered a harm due to Defendants' privacy violations, "a focus on economic loss is misplaced." Rather, the unlawful disclosure by Defendants of Plaintiffs' and the Class' legally protected information constitutes "a clear de facto injury." In re Horizon Healthcare, 846 F.3d at 636 (3d Cir. 2017).[7]

4. Defendants Unlawful Activity Also Violates The FTA Act, The Cable Communications Policy Act, and the Children's Online Privacy Protection Act

In addition, Defendants unlawful activity in this case also violates: (i) the Federal Trade Commision Act ("FTC Act");[8] (ii) the Subscriber Privacy Provision in the Cable Act;[9] and the Children's Online Privacy Protection Act.[10] See In re: Samsung Electronics Co., Ltd., 20 Federal Trade Commission, February 24, 2015 at 12-16 (attached as Exhibit 5 to the Complaint). See also Fed. Trade Comm'n v. Information Search, Inc., Civ. No. 1:06-cv-101099 *(March 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to the public . . ."). These violations by Defendants constitutes an additional violation by Defendants of the NJCFA.

---

[7] In Miller v. American Family Publishers, 284 N.J. Super. 67, 663 A.2d 643 (Ch. Div. 1995), the court stated "whenever a consumer has received something other than what he bargained for, he has suffered a loss of money or property" and thus an "ascertainable loss" under the NJCFA. Id. at 89. Alternatively, Plaintiffs have suffered ascertainable loss in this case because they intended to purchase a television only; Plaintiffs never bargained for the right of Defendants' to use their Smart TVs as a wiretap device in order to intercept, sore, and transmit private information to third parties, for profit.

[8] See 15 U.S.C. § 45 (2010). See also Fed. Trade Comm'n, FTC Policy Statement on Deception, available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm; Fed. Trade Comm'n, FTC Policy Statement on Unfairness, available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm

[9] See 47 U.S.C. § 631(b).

[10] See Children's Online Privacy Protection Act, 16 C.F.R. § 312.3 (2013).

These additional violations by Defendants are each separate, independent violations by Defendants of the NJCFA. See *Cox v. Sears Roebuck & Co., 138 N.J. 2, 13 647 A.2d 454 (N.J. 1994)* ("[p]roof of any . . . violation of a regulation will be sufficient to establish unlawful conduct under the [NJCFA]").

5. Plaintiff Has Complied with Federal Rule of Civil Procedure 9(b)

Plaintiffs' NJCFA claims also comply with Federal Rule of Civil Procedure 9(b) ("Rule 9(b)"). In order to satisfy Rule 9(b), plaintiffs must plead with particularity "the 'circumstances' of the alleged fraud in order to place the defendants on notice of the precise misconduct with which they are charged, and to safeguard defendants against spurious charges of immoral and fraudulent behavior." Sevillle Indus. Mach. Corp. v. Southmost Mach. Corp., *742 F.2d 786, 791 (3d Cir. 1984).* Plaintiffs may satisfy this requirement by pleading the "date, place or time" of the fraud, or through "alternative means of injecting precision and some measure of substantiation into their allegations of fraud." Id. (holding that a plaintiff satisfied Rule 9(b) by pleading which machines were the subject of alleged fraudulent transactions and the nature and subject of the alleged misrepresentations).

Here, Plaintiffs have placed Defendants on notice of the precise misconduct of which they complain, namely that Defendants - without informed consent - unlawful track and record consumers via their Smart TVs, and transmit this confidential, personally identifiable information to third parties, for profit. In their Complaint, Plaintiffs have thoroughly alleged the entire scheme perpetrated by Defendants from start to finish, including what occurred; where it occurred; how Defendants acquired private information; the partners Defendants used to perpetrate their scheme; and the complete model information, Smart TV features, place of purchase, location and type of usage, and much other detail respecting Plaintiffs' Smart TVs and their purchases. The Complaint also provides Defendants with New Jersey Plaintiff Cauley's Smart TV purchase receipt and the User Manual respecting her Smart TV. See Exhibit 2 and Exhibit 3 (attached to the Complaint).

Plaintiffs' allegations further showcase the full investigation of counsel in this case. Although not required to do so, Plaintiffs' Complaint cites almost fifty (50) authorities –

including FTC investigations and other reports; countless news and other articles; the materials and announcements of companies in privity with Defendants, such as Cognitive Networks; and experiences of users, which also detail and particularize Defendants misconduct in this case.

In addition, Plaintiffs also attach multiple exhibits to the Complaint and cite the extensive investigation conducted by The Electronic Privacy Information Center ("EPIC"), a leading consumer group before the FTC (which has also argued to the Supreme Court of the United States), which has independently investigated facts of this cas and even filed a related FTC complaint under oath.[11] This additional information also particularizes the facts surrounding this case.

Moreover, in this litigation, Defendants argued to the Court (against counsel for Plaintiffs' protests) that discovery could not be needed before their motion to dismiss was decided, and the Court therefore stayed all discovery in this litigation. However, all additional information and details concerning Defendants' unlawful conduct in this case is exclusively within the Defendants' possession and control. At this stage of the litigation, Defendants should not be rewarded by the Court for withholding the materials from Plaintiffs which would allow Plaintiffs to obtain even more precise details concerning Defendants' scheme to siphon and sell consumers' personal information.

Accordingly, Plaintiffs' have pled particularity under Rule 9(b) and the NJCFA claim should stand.

II. Plaintiffs' FDUPTA Claims Are Well-Pled

The Florida Deceptive and Unfair Trade Practices Act ("FDUPTA") prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." § 501.204(1), Fla. Stat. (2011). The term "trade or commerce" as used in section 501.204(1) is defined as "advertising, soliciting, providing, offering, or distributing whether by sale, rental, or otherwise, of any good or service, or any property ... or any other article, commodity, or thing of value, wherever situated." § 501.203(8), Fla. Stat. (2011). An unfair action under FDUTPA is an act that offends established

[11] See In re: Samsung Electronics Co., Ltd., 20 Federal Trade Commission, February 24, 2015 (attached to the Complaint as Exhibit 5).

public policy and one that is substantially injurious to consumers, unscrupulous, oppressive, unethical, or immoral. State v. Beach Blvd Automotive, Inc., 139 So. 3d 380, 390 (Fla. 1st DCA 2014) (upholding FDUPTA claim for the placement of a GPS tracking device without the consent of consumers on vehicles purchased at a car dealership) (citing PNR, Inc. v. Beacon Prop. Mgmt., Inc., 842 So.2d 773, 777 (Fla. 2003)). Deception occurs if there is a representation, omission, or practice that is likely to mislead consumers acting reasonably in the circumstances, to the consumers' detriment. Id.

FDUTPA is designed to protect "the rights of litigants" as well as "the rights of the consuming public at large." State, Office of Attorney General, Dept. of Legal Affairs v. Wyndham International, Inc., 869 So.2d 592, 598 (Fla. 1stDCA 2004). Simply stated, to be entitled to a remedy under FDUTPA, a plaintiff must show that the (a) defendant was engaged in a trade or business; (b) that the defendant engaged in unfair methods of competition or unfair or deceptive acts or practices involving trade or commerce; and (c) that the plaintiff suffered damages there from. The scope of the Act is broad and a **plaintiff need not prove fraud.** See State of Florida, Office of Attorney General, Dept. of Legal Affairs v. Tenet Healthcare Corp.,420 F.Supp.2d 1288 (S.D. Fla. 2005); Sony Corp. v. Discount Cameras & Computers, Inc., 2013 WL 4780077(M.D. Fla. 2013) (citing TracFone Wireless, Inc. v. GSM Group, Inc, 555 F.Supp.2d 1331 (S.D. Fla. 2008)).

As set forth in the Complaint and above (see supra Section B.2., *Unlawful Activity* discussion), Plaintiffs have satisfied each element of their FDUPTA claim by means of Defendants' unlawful scheme to secretly intercept, track, and record consumers, and then sell consumers' private, confidential information to third parties. Accord Burrows v. Purchasing Power, LLC, 2012 WL 9391827 (S.D. Fla. 2012) at 2 (citing Reilly v. Pluemarcher, 644 F.3d 38, 46 (3d Cir. 2011) (holding that, where a consumer's private information is taken by a defendant, economic damages are not needed to be shown because "that misuse private information or identity theft represents an actual injury."); Furmanite Am., Inc. v. T.D. Williamson, Inc., 506 F. Supp. 2d 1134, 1145-47 (M.D. Fla. 2007) (holding that FDUPTA extends to any person injured by a deceptive act or unfair practice, regardless of whether goods or services were bought or sold).

Furthermore, as discussed above, Defendants unlawful activity in this case also violates the FTC Act.[12] See In re: Samsung Electronics Co., Ltd., 20 Federal Trade Commission, February 24, 2015 at 12-16 (attached as Exhibit 5 to the Complaint). See also Fed. Trade Comm'n v. Information Search, Inc., Civ. No. 1:06-cv-101099 *(March 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to the public . . ."). Section 501.203, Florida Statutes, explicitly states that it is an unfair practice under FDUPTA to violate any of the rules promulgated by the FTC, such as "Trade Regulation Rules." See Fla. Stat. § 501.203(3)(a) (2016).

Accordingly, Defendants violations of the FTC Act constitutes additional, independent violations by Defendants of FDUPTA.

III. Plaintiffs' Statutory Privacy Claims Are Well-Pled

Plaintiffs have adequately pled their statutory privacy claims.

A. Plaintiffs' VPPA Claims Are Well Pled

Enacted in 1988, the Video Privacy Protection Act ("VPPA") provides that "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person . . ." 18 U.S.C. § 2710(b)(1); Video Privacy Protection Act of 1988, S. 2361, 100th Cong., 102 Stat. 3195 (1988) (emphasis added). The Act allows consumers "to maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers." S. Rep. No. 100-599 at 8 (1988). The VPPA also protects consumers by requiring that their consent be obtained before their personal video-viewing histories can be divulged. Id. Defendants seek to dismiss Plaintiffs' VPPA claims, arguing that they are not "video tape service provider[s]," that Plaintiffs are not "consumer[s]" as defined by the statute, and that Defendants

[12] See 15 U.S.C. § 45 (2010). See also Fed. Trade Comm'n, FTC Policy Statement on Deception, available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm; Fed. Trade Comm'n, FTC Policy Statement on Unfairness, available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm

do not disclose "personally identifiable information." Each argument misreads the VPPA; the instant Complaint; and the Third Circuit's (and other courts') interpretation of the statute.

1. Defendants Are "Video Tape Service Providers"

Defendants deliver through Smart TV software streaming video directly to consumers homes through the software that Defendants developed for its Smart TVs. Compl. ¶¶ 34-35. Using Defendants' platforms, the user can select videos from various video libraries, including Hulu's, Amazon's and Netflix's, for instant delivery. Compl. ¶¶ 36, 47 [13] By using Defendants' video-delivery software service, Defendants collect certain private information about the user. Compl. ¶¶ 38-67.

Against this backdrop, Plaintiffs have properly alleged that each Defendant qualifies as a "video tape service provider" because it is a "person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials[.]" 18 U.S.C. § 2710. That is, the Complaint precisely alleges that each Defendant is not merely a television manufacturer; they also clearly provide consumers with a service: the delivery of streaming video (i.e., "similar audio visual materials") through their Smart TV platforms. Indeed, Plaintiffs (like virtually every purchaser of a Smart TV) purchased their Smart TVs in part because Defendants' technology brings the video rental store into the home, allowing Plaintiffs to access video on demand through Defendants' Smart TV interface.

Defendants contend they are not video tape service providers under the VPPA. However: The plain text of the statute provides otherwise. As an initial matter, Congress's use of a disjunctive list (i.e., 'engaged in the business . . . of . . . rental, sale, or delivery') unmistakably indicates that Congress intended to cover more than just the local video rental store. Indeed, lest the word 'delivery' be superfluous, a person need not be in the business of either renting or selling video content for the statute to apply.

[13] In this regard, Defendants compete directly with other video delivery services, such as Roku. See https://article.wn.com/view/2018/01/17/Roku_Introduces_New_Metrics_for_OTT_Advertising_Campaigns/

Further, Congress's use of the phrase 'similar audiovisual materials' indicates that the definition is medium-neutral; the defendant must be in the business of delivering video content, but that content need not be in a particular format. In re Vizio, Inc., 238 F. Supp. 3d 1204, 1221. See also In re Hulu Privacy Litig., No. C 1103764 LB, 2012 WL 3282960, at *5 (N.D. Cal. Aug. 10, 2012). Accord In re Nickelodeon Cons. Priv. Litig., 827 F.3d at 290 (3d Cir. 2015).[14]

As the statutory text supports Plaintiffs' position -- not Defendants' -- so does the legislative history. The VPPA was of course enacted before this type of technology existed, but "Congress was concerned with protecting the confidentiality of private information about viewing preferences regardless of the business model or media format involved." Hulu, 2012 WL 3282960, at *6 (emphasis added). Congress may not have imagined the technology Defendants have developed to deliver streaming video through licensing agreements with content providers like Hulu, but it "cast such a broadly inclusive net in the brick-and-mortar world, [that there is] no reason to construe its words as casting a less inclusive net in the electronic world when the language does not compel that we do so." See Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 488 (discussing "subscriber").

Thus, in addition to the fact that, on its face, each Defendants clearly provide an in-home video delivery service to consumers, Congress's choice of language in defining video tape service provider also fairly brings Defendants' video-delivery service within the VPPA, and therefore "it is unimportant that the particular application may not have been contemplated by the legislators." Barr v. United States, 324 U.S. 83, 90 (1945). Accordingly, the VPPA's protections plainly do apply to a business that runs a video-delivery service through software designed to bring the video-rental store into the home—which is precisely why each Defendant is a qualifying "video tape service provider."[15]

---

[14] "[W]hen [a] statute's language is plain, the sole function of the courts – at least where the disposition required by the text is not absurd – is to enforce it according to its terms." Lamie v. U.S. Tr., 540 U.S. 526, 534 (2004) (quoting Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A., 530 U.S. 1, 6 (2000). "The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which the language is used, and the broader context of the statute as a whole." Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997).

[15] Companies like Hulu, which are accessible through Defendants' video-delivery software, are not the only "video tape service providers" within the arrangement. The VPPA simply asks whether an interstate business is engaged in the delivery of "similar audio visual materials," which includes streaming video.

2. Plaintiffs Are Subscribers And Hence Consumers

Next, Defendants argues that Plaintiffs are not "consumers" under the VPPA. The statute defines "consumer" to include a "subscriber" of goods or services from a video tape service provider. 18 U.S.C. § 2710(a)(1). Though the word subscriber is not defined therein, its ordinary meaning includes one who receives electronic texts or services by subscription. Yershov, 820 F.3d at 487.

In Yershov, the First Circuit held that an individual who accesses news and entertainment media content, including videos, through a proprietary mobile software application on his mobile phone qualifies as a "subscriber" within the meaning of the VPPA. The app was free, but the court rejected the argument that monetary payment is necessary to qualify as a subscriber. 820 F.3d at 487. Instead, it found that the use of the mobile app generated information about that user that the defendant collected, and this was sufficient to establish a subscriber relationship. Id.; see also Hulu, 2012 WL 3282960, at *8 (concluding plaintiffs were subscribers of Hulu, notwithstanding that they watched videos on Hulu for free, in part because Hulu collected their data in exchange for viewing).[16]

Simply put, Plaintiffs here used Defendants' proprietary Smart TV platform to watch video, and Defendants collected and sold (and continue to collect and sell) Plaintiffs' and consumers' personal data when they do, such as computer addresses and the addresses of other electronic items connected to Wifi, and what, where and when consumers watch -- which can be then be used (and are used) by Defendants to reveal Plaintiffs' electronic location and the location of other devices connected to Plaintiffs' Wifi (i.e., geolocation data). Compl. ¶¶ 38, 49,

---

See In re Hulu Privacy Litig., 2012 WL 3282960, at *5-*6 (N.D. Cal. Aug. 10, 2012) (holding Hulu qualified as a "video tape service provider" because it helped deliver television and movies through the Internet for free). Instead, under a plain reading of the statute, any company that provides this service must obtain informed consent before disclosing individuals' personal viewing-histories and confidential, identifying information.

[16] In Yershov, the First Circuit concluded that a consumer need not make a monetary payment in return for a mobile application to be considered a "subscriber." 820 F.3d 482, 488-89 (1st Cir. 2016). Instead, the plaintiff's provision of personal information in return for the defendant's video content was sufficient consideration for the plaintiff to be a "subscriber." Id. at 489. See also In re Vizio, Inc., 238 F. Supp. 3d 1204.

57, 154. Defendants also collect this data so that they can push personalized ads to their devices as well as consumers' other devices. Compl. ¶¶ 45-47. "[A]ccess was not free of a commitment to provide consideration in the form of that information, which was of value to" Defendants. See Yershov, 820 F.3d at 489.

And it was not free in a different sense: Defendants sell Smart TVs with this "streaming video" technology (at a premium) in order to allow consumers to have regular, and easy, access to video delivery services in their homes. Ironically and absurdly, all along Defendants were and are secretly using those same delivery services to reap millions of dollars off the personal, private information from unsuspecting consumers.

In these ways, Plaintiffs have alleged a sufficient relationship with Defendants' video delivery services, such that Plaintiffs are clearly "subscribers" under the VPPA.

3. Defendants Disclosed Plaintiffs' and Class Members' "Digital Identities" Constituting Personally Identifiable Information

The VPPA provides that "the term 'personally identifiable information' includes information which identifies a person . . ." § 2710(a)(3) (emphasis added). Unlike other definitions of "personally identifiable information" which list specific types of data as qualifying, this is an example of a "standard" which is "open rather than closed in nature" and "can evolve and remain flexible in response to new developments." Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814 (2011). That Congress chose to define "personally identifiable information" in terms of a standard is evident from its use of the word "includes." This word "normally implies that the proffered definition falls short of capturing the whole meaning." Yershov, 820 F.3d at 486; see also United States v. Gertz, 249 F.2d 662, 666 (9th Cir. 1957) ("The word 'includes' is usually a term of enlargement, and not of limitation."). The legislative history confirms this reading. Id. (noting "official Senate Report expressly stating that the drafters' aim was 'to establish a minimum, but not exclusive, definition of personally identifiable information.'" (quoting S. Rep. No. 100–599, at 12)).

Congress's approach makes great sense for two reasons. For one, "many types of information other than aname can easily identify a person." 820 F.3d at 489.[17] It can depend on the context: "*[W]hen a football referee announces a violation by 'No. 12 on the offense,' everyone with a game program knows the name of the player who was flagged*." Id. (emphasis added). For another, the ability of any given information to identify individuals may change over time. 86 N.Y.U. L. Rev. at 1836.

Here, Plaintiffs allege that Defendants video-streaming platforms disclose substantial, extensive information about Plaintiffs' and consumers' digital identities; namely, consumers' video-viewing history, consumers' computer addresses, and information about other devices connected to the same Wifi network. Compl. ¶¶ 43-50. That alone satisfies the VPPA pleading standard laid down by the Third Circuit in In re Nickelodeon Cons. Priv. Litig., 827 F.3d at 290 (3d Cir. 2015). Moreover, the court in Vizio (a case with allegations virtually identical to this one)– applied the standard laid down by the Third Circuit in Nickelodeon and explained why Plaintiffs' VPPA claims should be upheld:

> The Court need not disagree with *In re Nickelodeon* because Plaintiffs allege that Vizio's Inscape platform discloses even more about their digital identities—in particular, consumers' MAC addresses and information about other devices connected to the same network. Plaintiffs allege that MAC addresses are frequently linked to an individual's name and can be used to acquire highly specific geolocation data. (Compl. ¶¶ 69-71.) MAC addresses allegedly can also identify a person when combined with Vizio's disclosure of consumers' IP addresses, zip codes, product model numbers, hardware and software versions, chipset IDs, and region and language settings. (Id. ¶¶ 72-79.) Besides collecting and disclosing extensive information regarding consumers' Smart TVs, Vizio supposedly collects and discloses information about all other devices connected to the same network. (Id. ¶¶ 63, 72.)

[17] "Congress contemplated that the Act would protect more than just a person's name or physical address." See also In re Vizio, Inc., 238 F. Supp. 3d 1204, 1224. Besides collecting and disclosing extensive information regarding consumers' Smart TVs, Plaintiffs allege that Defendants collect and disclose information about all other devices connected to the same network. See, e.g., Compl. ¶¶ 43-53.

In re Vizio, Inc., 238 F. Supp. 3d 1204, 1224. See also Yershov, 820 F.3d at 489.

In the instant case, Plaintiffs have made similar allegations, and the same reasoning applies.

Plaintiffs' allegations here also detail how this personal information taken by Defendants links viewing data to specific individuals, including the creating by Defendants of a digital "fingerprint" of every user in a home and Defendants' ability to scan a users' Wifi network. Compl. ¶¶ 43-50. Plaintiffs describe how addresses are unique to Plaintiffs' Smart TVs and consumers' other electronic devices. Id. Plaintiffs allege Defendants disclose this data for not only the Smart TVs themselves, but all media sources connected to consumers' Wifi. Id. These allegations also plausibly state a claim under the VPPA. Nickelodeon, 827 F.3d at 290. See also Yershov, F. Supp. 3d at 135; In re Vizio, Inc., 238 F. Supp. 3d 1204, 1225. 12

Further, The First Circuit in Yershov concluded that personally identifiable information extends beyond a person's name to embrace "information reasonably and foreseeably likely to reveal which . . . videos [the plaintiff] has obtained." In re Vizio, Inc., 238 F. Supp. 3d 1204, 1224 (citing Yershov, 820 F.3d at 486).[18]

Defendants argue that this is not what they are doing and ask the Court to hold that the confidential and identifying personal information about consumers that Defendants steal, store, and sell to third parties (i.e., specific information that identifies *what* a user watches; *how long* a user watches; and *where* they watch videos, as Plaintiffs allege) does not violate the VPPA as a matter of law. As Defendants know and explained in detail above, this factual argument and inquiry – a dispute of scientific fact – and is entirely improper in a technology case at the pleadings stage. See E.digital Corp. v. Toshiba Am. Info. Sys., Inc., 2014 WL 12516081, at *3 (S.D. Cal. July 10, 2014). "[S]uch arguments are better suited for a motion for summary judgment on a more developed record." E.digital Corp., 2014 WL 12516081, at *3. See also In re Vizio, Inc., 238 F. Supp. 3d 1204, 1225.

At the pleadings stage, the Court must accept as true all allegations of material facts that are in the complaint and must construe all inferences in the light most favorable to the non-moving party." In re Horizon Healthcare Servs., Inc. Data Breach Litig., 846 F.3d 625 (3d

[18] Of course, discovery will hopefully allow for details concerning how extensive Defendants' were collecting and disclosing (and are currently collecting and disclosing) private consumer information and information about all other devices connected to consumers' Wifi networks.

Cir. 2017). As such, the Court should also not accept Defendants' offer to engage in judicial fact finding or make sweeping determinations as a matter of law on this Motion to Dismiss. Yershov, 104 F. Supp. 3d at 145 ("the factual record would need to be developed before concluding that an Android ID is not PII"); In re Hulu Privacy Litig., 2012 WL 3282960, at *7 (N.D. Cal. Aug. 10, 2012) ("Plaintiffs do not have to plead their evidence to give fair notice of their claims."); See also In re Vizio, Inc., 238 F. Supp. 3d at 1225-1226 ("Plaintiffs will have to demonstrate that Defendants' disclosures are 'reasonably and foreseeably likely to reveal' what video content Plaintiffs have watched. . . .. But this is a factual inquiry ill-suited for resolution on a motion to dismiss.") (emphasis added).

Plaintiffs have clearly alleged enough facts to plausibly demonstrate that Defendants have unlawfully disclosed, and are continuing to unlawfully disclose Plaintiffs' and the Class' private, confidential information. "Having informed [Defendants] of the factual basis for their complaint, [Plaintiffs] were required to do no more to stave off threshold dismissal for want of an adequate statement of their claim." See Johnson v. City of Shelby, Miss., 135 S. Ct. 346, 347 (2014). Accordingly, it would not be appropriate to conclude that "the linkage of information to identity" here is "too uncertain." Yershov, 820 F.3d. at 486.

For the reasons stated above, Plaintiffs VPPA claims should stand.

4. Defendants Know That Information They Disclose Identifies Individual Viewers And Their Location

Defendants know that individuals and their viewing histories can be, and are easily being, identified and linked by the information Defendants disclose. In fact, individuals can be identified with far less information than what Defendants disclose. A groundbreaking study published in 2000 revealed that three pieces of information—zip code, birth date (including year), and sex—uniquely identified 87 percent of the U.S. population. Other studies have found similarly high rates of identification. Compl. ¶ 74.

At least since 2006, video service providers have known that the disclosure of viewing data not associated with individual names can nevertheless be associated with specific individuals. That year, Netflix released a data set representing the movies rated by over 480,000 Netflix customers and the date each rating was given. In an apparent effort by Netflix to anonymize the data, the company replaced customers' names with unique numbers and did not

include addresses, phone numbers, or other direct identifiers. Compl. ¶ 75.

Netflix released the data "as part of its Netflix Prize contest, through which researchers competed to improve the algorithm Netflix uses to recommend movies to its subscribers. Netflix's algorithm takes into account past viewing habits and movie preferences of each of its subscribers." Id. Following the release of this data set, two researchers at the University of Texas announced that it was possible to identify a significant number of subscribers based on the data set released. The researchers concluded -- using 2008 technology:

> We demonstrate that an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber's record in the dataset. Using the Internet Movie Database as the source of background knowledge, we successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information. .. . . [Using publicly-available movie reviews posted by Netflix subscribers on the popular site IMDb (www.imdb.com)], one could determine all of the Netflix movies that a subscriber had rated for a given period of time.

Compl. ¶ 76-77

Thus, Defendants thus know that third parties to whom they disclose this information, which includes its partners, can and do connect these dots. And using 2018 technology, so can the ordinary person. The linkage between viewing data and individuals is firm and readily foreseeable to Defendants, in particular because the information it discloses is effectively a correlated look-up table, complete with geolocation data. Compl. ¶ 78.[19]

[19] Retail analytics firms have used computer and device addresses to pinpoint customer locations— a practice which the Federal Trade Commission ("FTC") has investigated. See *How to Trace an IP Address to a PC & How to Find Your Own*, https://www.makeuseof.com/tag/how-to-trace-an-ip-address-how-to-find-your-own-nb/

B. Plaintiffs' Wiretap Act Claims Are Well-Pled

The Wiretap Act prohibits "interceptions" of electronic communications. 18 U.S.C. § 2510. It defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." § 2510(4). The "contents" of a communication are defined as "any information concerning the substance, purport, or meaning of that communication." § 2510(8). Plaintiffs' complaint alleges enough facts to state a Wiretap Claim that is plausible on its face.

1. Defendants "Intercepted" Electronic Communications.

In order for a communication to be "intercepted" under the Wiretap Act, the communication must be captured contemporaneous with its transmission. See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) ("intercept" means "consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.'") (citations omitted). Here, Plaintiffs' Complaint specifically pleads that Defendants captured (and continue to capture) real-time viewing behavior data from consumers by means of their Smart TVs. Compl. ¶¶ 44. Moreover, consumers' information was obviously acquired by Defendants during transmission of the programming to Defendants' Smart TVs. How else could Defendants monitor and acquire that information?

These allegations of real-time acquisition are sufficient to withstand a motion to dismiss. See In re Carrier IQ, Inc., 78 F. Supp. 3d 1051, 1078-79 (N.D. Cal. 2015) (denying motion to dismiss Wiretap Act claim where the complaint "references and quotes from a media interview with a Carrier IQ executive" who stated information was provided in real time and holding that the statement "further suggest[s] that the Carrier IQ Software operates contemporaneously with transmissions.");[20] Luis v. Zang, 833 F.3d 619, 630-31 (6th Cir. 2016) (interception sufficiently pled where plaintiff alleged that the product in question "immediately and instantaneously rout[e]s the intercepted communications to their . . . servers" in "near real-time," and attaching marketing materials to his complaint that "directly support[ed] an inference of contemporaneous

[20] Carrier IQ correctly distinguished cases involving technology with allegations that the relevant communications were intercepted in real-time, which, is precisely what the Complaint pleads here. 78 F. Supp. 3d at 1078.

transmission.").[21] Accord In re Google Inc., 806 F.3d 125, 135-140 (3rd Cir. 2015); Campbell v. Facebook, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014).

Thus, the Complaint plausibly and sufficiently alleges that Defendants took (and continue to take) Plaintiff's and consumers' confidential, identifying information in real time while that information was (and is) in transit to Defendants' Smart TVs. Since the allegations in the Complaint must be accepted as true at this stage, Plaintiffs have sufficiently alleged interception.

2. Defendants Intercepted The "Contents" Of Communications, As Viewing History And Watching Preferences Are "Contents"

Plaintiffs allege that Defendants intercepted (and continue to intercept) communications between them and cable and satellite providers, streaming devices, and media sources that connect via external input to their Smart TVs and consumers Wifi. Compl. ¶ ¶ 38-67. Plaintiffs allegations detail that, amongst other confidential, identifying information, Defendants secretly learned what movies and television Plaintiffs and other consumers watch, when they watch, where they watch, and for how long - and then Defendants sold that private information to third parties for profit. Id. See also Exhibit 4 to the Complaint. Just as a request in person to a video store clerk for a specific movie is the substance of the message itself, so too are Plaintiffs' requests for programming through their Smart TVs and other devices, which Defendants intercept. Accord In re Zynga Privacy Litig., 750 F.3d 1098, 2014 WL 1814029, at *9 (9th Cir. 2014) ("Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging that search term to a third party could result in disclosure of contents.").[22]

---

[21] Notably, Plaintiffs here have likewise attached marketing materials to their Complaint which clearly and directly supports the exact same inference. See Automatic Content Software Platform materials (attached to the Complaint as Exhibit 4).

[22] In Zynga, the court held that the portion of a webpage request message that provides the address of the webpage from which the request originated did not meet the Wiretap Act's definition of "contents" because it included only basic identification and address information. The court, however, was careful to say, "Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a [Uniform Resource Locator (URL)] containing that search term to a third party could amount to disclosure of the contents of a communication." 750 F.3d 1098, 1108-09 (emphasis added).

As alleged in the Complaint, when consumers request a particular program, and Defendants intercept that communication, they are learning specific, highly sensitive information about consumers and consumers' personal interests. Defendants then sell this confidential, identifying information to target Plaintiffs with ads about their interests – even on devices other than the Smart TV itself. See, e.g., Compl. ¶¶ 5, 42.

As such, Defendants intercepted, and continue to intercept, under the Wiretap Act.

3. Plaintiffs' Wiretap Claims Should Stand

In short, Plaintiffs allege that Defendants' technology tapped into transmissions to Smart TVs in real time and lifted samples of the content being transmitted so that Defendants could determine what Smart TV-users watch, where they watch, and when they watch. Plaintiffs also allege that Defendants match data and create "fingerprints" of the samples of consumers' watching history and viewing habits. It does not matter whether the video samples taken by Defendants were fragmentary bits of audio or visual data as opposed to lengthier, wholesale recordings, which will be showcased during discovery in this case. The Wiretap Act prohibits the interception of any information concerning the substance of an electronic communication. 18 U.S.C. § 2510(8) (defining "contents"). There is no safe harbor under the Wiretap Act for interceptions of only parts, or samples of transmissions, and there is no safe harbor for Smart TVs.

Accordingly, Defendants' motion to dismiss Plaintiffs' Wiretap Act claims should be denied.

IV. Defendants' Statute Of Limitations Argument Is Absurd And Incorrect

Defendants' claim that Plaintiffs and the Class should not have their day in Court, and Defendants' should be able to evade responsibility for their alleged misconduct, because they are barred by the statute of limitations. Their argument, however, is absurd, as Plaintiffs have alleged an ongoing violation here. That is, Defendants are continuing to engage in the illegal conduct complained of -- even right now!

Accordingly, each time Defendants steal, collect, transmit, sell and/or otherwise use private and/or identifying information about consumers, they violate both statutes. Plain in simple, on its face, there is no valid statute of limitations argument to the Complaint, at all.

Moreover, as alleged by Plaintiffs, concrete news concerning Defendants' misconduct here was first corroborated with "hard evidence" and then made open and available to the public at large at the time of Wikileaks' startling revelation on March 7, 2017, when Wikileaks reported that it had obtained proof in the form of "hard evidence" and government documentation that Smart TVs were in fact being used by outside parties to spy on consumers' private conversations, even when those Smart TVs were supposedly turned off. See Compl. at note 5. It was that announcement that made Plaintiffs and virtually all consumers throughout the world aware of Defendants' misconduct and specifically, the seriousness of the situation and the need to take legal action against Defendants in this case. Accordingly, Defendants' contention that Plaintiffs' claims are time barred must fail. These are continuing, ongoing violations by Defendants, and Plaintiffs were first able to reasonably confirm the substance of the allegations in the Complaint in March 2017.

V. Both Defendants Have Engaged In An Unlawful Industry Standard

Defendants also engaged in an illegal industry standard to intercept and sell consumers' private information by means of their Smart TVs. Defendants had licensing agreements with the same outside companies at various times, and their data collection and consumer-information mining process was – and is – an illegal industry standard that each Defendant reaps many, many tens or hundreds of millions of dollars from. Plaintiffs have alleged that, there is so much money at stake here, that both of the TV-manufacturer Defendants engaged in virtually the exact same conduct.[23]

For Defendants to try to use their participation in their own illegal industry standard as a defense to the conduct asserted against them by Plaintiffs in this case is ludicrous. Moreover, Plaintiffs' counsel can ascertain no other logical business purpose for the outside data recognition companies used by Defendants and cited by Plaintiff, than for exactly what

[23] See Compl. at note 20 (*citing* Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lgvizio-smart-tvs-watch-everything-you-watch/index.htm) ("Precise data about consumers TV viewing habits is big business. Revenues for audience-measurement company Nielsen surpassed $6 Billion last year.") (emphasis added).

Defendants allege about each Defendant in the Complaint. As the old adage goes - "a picture is worth a thousand words" - so counsel for Plaintiffs respectfully asks this Court to review Exhibit 4 to Complaint to see that the outside data companies used by Defendants were setting the illegal standards for Defendants to follow, which Defendants happily did.

SUMMARY

For the reasons stated above, Defendants' motion to dismiss Plaintiffs' Amended Class Action Complaint should be denied in its entirety.

DATED: January 25, 2019

Respectfully submitted,

BERMAN CLASS LAW
By: /s/ Mack Press
421 Union Avenue
Peekskill, NY 10566
mack@mackpress.com
(516) 330-7213